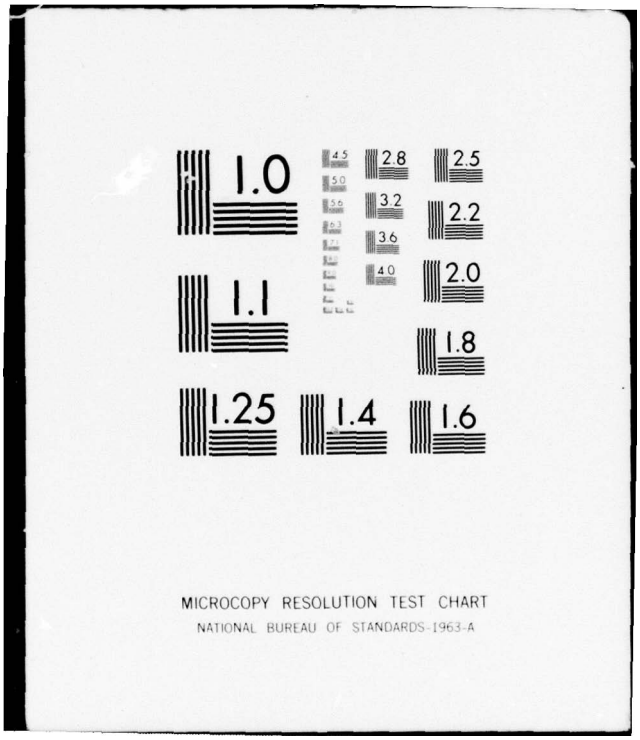
AD-A039 574 YALE UNIV NEW HAVEN CONN DEPT OF COMPUTER SCIENCE F/G 12/1
ON STRUCTURE PRESERVING REDUCTIONS.(U)
DEC 76 R J LIPTON, N LYNCH N00014-75-C-0752
UNCLASSIFIED RR-85 NL

| OF |
AD
A039574

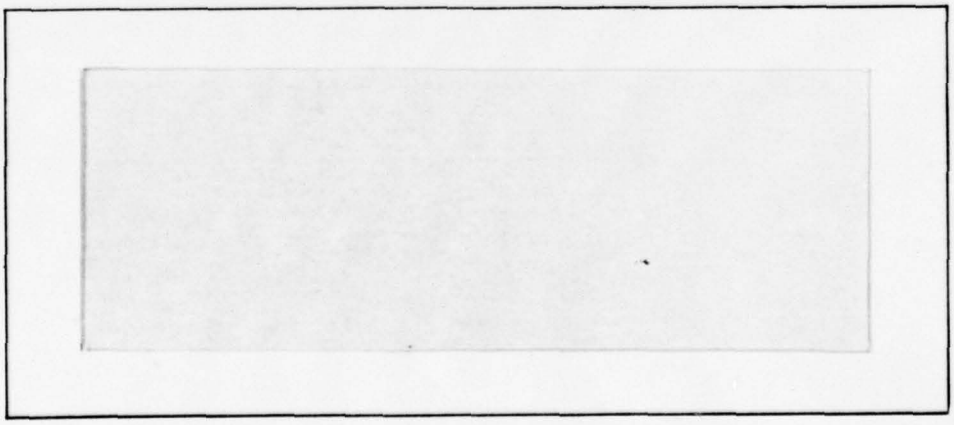
END

DATE
FILMED
6-77


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
7.1
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD A039574

DDC
MAY 17 1977
C



DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

AD No.
DDC FILE COPY.

YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

DDC
RECEIVED
MAY 17 1977
C

(14) RR-85

(11) Dec 76

(12) 19 p.

(6) On Structure Preserving Reductions.

(10) Nancy Lynch[1] and Richard J. Lipton[2]

(9) Research Report, #85

ACCESSION for
NTIS White Section
D C Buff Section
UNANNOUNCED
JUSTIFICATION
BY
DISTRIBUTION/AVAILABILITY CODES
Dist. AVAIL. and/or SPECIAL
A

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

[1] University of Southern California
Florida International University

[2] Yale University

This work was supported in part by the National Science Foundation under Grant DCR 92373, and also in part by the Office of Naval Research under Grant N00014-75-C-0752,

(15) NSF-DCR-92373

407 051

Abstract:

The concept of reduction between problems is strengthened. Certain standard problems are shown to be complete in the new and stronger sense. Applications to the number of solutions of particular problems are presented.

keywords: reductions, polynomial time, logspace, complete sets.

1. Introduction

One of the most striking features of a large number of the known reductions of one problem to another [K] is that they often preserve a great deal more than they have to. More precisely, suppose that A is many-to-one polynomial time reducible to B where A and B are, as usual, subsets of Σ^* for some finite alphabet Σ. Then all that is required in the usual definition is that

(*) $\forall x \in \Sigma^*, x \in A$ if and only if $f(x) \in B$,

where f(x) is some polynomial time computable function. Essentially (*) states that x has a solution exactly when f(x) has a solution. It appears, however, that quite often x and f(x) are more closely related than this.

This imprecise intuitive feeling that reductions often preserve additional structure is the subject of this paper. Our principle result is the introduction of a new kind of reduction and a proof that some standard complete problems are also complete in our strong sense.

The notion that reduction preserves additional structure also appears in Simon [Si]. His main result is that a number of problems are still equivalent when (*) is strengthened to:

x has the same number of solutions as f(x).

He calls these equivalent problems parsimonious. There is a difficulty with these results, however; it is not clear what it means for x to have k solutions when A is an arbitrary set. Clearly, either x is in A or it is not. Simon avoids this difficulty by working only with well known and specific problems. In these cases it is reasonable to assume that "x has k solutions" is a meaningful concept. We take an alternative approach. The main virtue of this approach is that it allows us to work with arbitrary problems, and thus we can prove the existence of complete sets.

2. New Definition of Reduction

The key idea of our new reduction is that we will focus our attention on relations rather than on sets. Roughly, suppose that

$$\forall x \in \Sigma^*,\ x \in A \text{ if and only if } \exists y\ R(x,y).$$

The intuitive concept that "x is an instance of A with k solutions" can be more precisely rendered by "there are k y's such that R(x,y) is true." There are, however, several interesting difficulties in making this rough idea work correctly. In this direction the next definition is the key.

Definition: A combination machine is a Turing machine with two read-only input tapes with end-markers, the first 2-way and the second 1-way, a 2-way read-write worktape and a 1-way write-only output tape. A combination machine is logspace (polynomial time) if it always halts and runs within worktape space logarithmic (within time polynomial) in the length of the first input.

As remarked in [LiL], a set A is in NL, the class of nondeterministic logspace sets (NP, the class of nondeterministic polynomial time sets) if and only if there exist a polynomial p and a relation R such that

$$x \in A \Leftrightarrow (\exists y)[|y| \leq p(|x|) \wedge R(x,y)],$$

and R is computable by a logspace (polynomial time) combination machine.

Now let R and S be arbitrary binary relations, and let r and s be polynomials. Then we will define reducibility $\leq^L (\leq^P)$ between (R,r) and (S,s) as follows:

$(R,r) \leq^L (\leq^P)(S,s)$ provided there exists an f and g such that

1. f is a function computable by a deterministic logspace (polynomial time) transducer 2-way on its input;

2. g is a function computable by a logspace (polynomial time) combination machine;

3. $\forall x,y \in \Sigma^*$,

$$\left[R(x,y) \wedge |y| \leq r(|x|)\right] \text{ implies } \left[S(f(x),g(x,y)) \wedge |g(x,y)| \leq s(|f(x)|)\right];$$

4. g is 1-1 in the sense that $\forall x,y_1,y_2 \in \Sigma^*$,

$$\left[R(x,y_1) \wedge R(x,y_2) \wedge |y_1| \leq r(|x|) \wedge |y_2| \leq r(|x|) \wedge g(x,y_1) = g(x,y_2)\right] \text{ implies } y_1 = y_2;$$

5. g is onto in the sense that $\forall x,z \in \Sigma^*$,

$$\left[S(f(x),z) \wedge |z| \leq s(|f(x)|)\right] \text{ implies } \left[\exists y \ |y| \leq r(|x|) \wedge R(x,y) \wedge g(x,y) = z\right].$$

This definition, while at first appearing to be quite complex, is actually a natural extension of the usual one. In order to see this, observe that the usual definition states that A is logspace (polynomial time) reducible to B for A and B which are expressed by

$$A = \{x \mid \exists y \quad |y| \leq r(|x|) \wedge R(x,y)\} \quad \text{and}$$

$$B = \{x \mid \exists y \quad |y| \leq s(|x|) \wedge S(x,y)\} \quad \text{provided}$$

$$\left[\exists y \quad |y| \leq r(|x|) \wedge R(x,y)\right] \iff \left[\exists y \quad |y| \leq s(|f(x)|) \wedge S(f(x),y)\right],$$

where f is some logspace (polynomial time) transduction. Our main idea is to strengthen this condition by putting into 1-1 correspondence specific witnesses to the two existential quantifiers.

Note that according to our definitions, if $(R,r) \leq^L (\leq^P)(S,s)$ via f and g, then for any x,

$$\left| \{y \mid |y| \leq r(|x|) \wedge R(x,y)\} \right| = \left| \{y \mid |y| \leq s(|f(x)|) \wedge S(f(x),y)\} \right|.$$

Proposition 1: $\leq^L (\leq^P)$ is transitive.

Proof: We first consider $\leq^L$. We need only show that if $(R,r) \leq^L (S,s)$ via f,g and $(S,s) \leq^L (T,t)$ via f', g' then $(R,r) \leq^L (T,t)$ via

$f'' = \lambda x[f'(f(x))]$ and

$g'' = \lambda x,y[g'(f(x),g(x,y))]$.

First, f" is a logspace transduction; this follows by standard arguments [SM]. Next, we must show that g" is computable by a logspace combination machine. We compute $g''(x,y)=g'(f(x),g(x,y))$ as follow

> Simulate g'. The only difficulty is in obtaining the appropriate bits of the inputs to g' as needed. The first input is easy: in order to compute the ith bit of f(x) we need only simulate f(x) from the beginning until it outputs the ith bit. This works since x is 2-way; a counter must be maintained for i. The second input is more difficult. In order to compute the ith bit of g(x,y) we simply simulate g(x,y) until it outputs the ith bit. The key is that g' asks for these bits in the same order as produced in the computation of g(x,y); thus, in the simulation of g(x,y) it suffices to have y on a 1-way tape. No counter need be maintained for i in this case.

We next show

3. $\left[R(x,y) \wedge |y| \leq r(|x|)\right]$ implies $\left[T(f''(x),g''(x,y)) \wedge |g''(x,y)| \leq t(|f''(x)|)\right]$.

We have, of course, that

$$\left[R(x,y)\wedge|y| \leq r(|x|)\right] \text{implies} \left[S(f(x),g(x,y))\wedge|g(x,y)| \leq s(|f(x)|)\right]$$

and that

$$\left[S(z,w)\wedge|w| \leq s(|z|)\right] \text{implies} \left[T(f'(z),g'(z,w))\wedge|g'(z,w)| \leq t(|f'(z)\right].$$

Thus

$$\left[R(x,y)\wedge|y| \leq r(|x|)\right] \Rightarrow \left[S(f(x),g(x,y))\wedge|g(x,y)| \leq s(|f(x)|)\right]$$
$$\Rightarrow \left[T(f'(f(x)),g'(f(x),g(x,y))) \wedge |g'(f(x),g(x,y))| \leq t(|f'(f(x))|)\right],$$

as needed.

Next, we show

4. $\left[R(x,y_1)\wedge R(x,y_2)\wedge|y_1| \leq r(|x|)\wedge|y_2| \leq r(|x|) \wedge g''(x,y_1) = g''(x,y_2)\right]$ implies $y_1 = y_2$.

Assume

$$R(x,y_1)\wedge R(x,y_2)\wedge|y_1| \leq r(|x|)\wedge|y_2| \leq r(|x|)\wedge g''(x,y_1)=g''(x,y_2).$$

Now it follows that

$$S(f(x),g(x,y_i)) \text{ and } |g(x,y_i)| \leq s(|f(x)|) \text{ for } i = 1,2.$$

Since $g'(f(x),g(x,y_1)) = g'(f(x),g(x,y_2))$, and g' is 1-1, we can conclude that $g(x,y_1) = g(x,y_2)$. Now since g is 1-1 we finally conclude that $y_1 = y_2$, as needed.

Finally, we must prove

5. $\left[T(f''(x),z)\wedge|z| \leq t(|f''(x)|)\right]$ implies $\left[\exists y\ |y| \leq r(|x|)\wedge R(x,y) \wedge g''(x,y) = z.\right]$

Assume that $T(f''(x),z)\wedge|z| \leq t(|f''(x)|)$. Since g' is onto there is a w such that $|w| \leq s(|f(x)|)$ and $S(f(x),w)$ and $g'(f(x),w)=z$. Again since g is onto there is an $|y| \leq r(|x|)$ such that $R(x,y)$ and $g(x,y) = w$. Thus

$g''(x,y)=g'(f(x),g(x,y)) = g'(f(x),w) = z$, as needed.

Thus, $\leq^L$ is transitive. The corresponding proof for $\leq^P$ is similar and simpler. ⊠

Definition: (S,s) is L-complete (P-complete) if S is a relation computable by a logspace (polynomial time) combination machine, s is a polynomial, and for all (R,r), where R is computable by a logspace (polynomial time) combination machine and r is a polynomial,

$$(R,r) \leq^L (\leq^P) \quad (S,s).$$

It is not difficult to show that if (S,s) is L-complete (P-complete), then

$\{x\ \exists y\ |y| \leq s(|x|)\wedge S(x,y)\}$ is complete in NL (NP) according to the more usual definitions.

Let SAT(x,y) be "x is a conjunctive normal form Boolean formula and y is an assignment of true or false to the variables of x making x true".[K]. SAT is clearly computable by a polynomial time combination machine. Let $s(n) = n$.

Proposition 2: (SAT,s) is P-complete.

Proof: Let R be a relation computable by a polynomial time combination machine M and let r be a polynomial. We will construct a nondeterministic Turing machine M' from M and r as follows:

M' on input x simulates M on inputs of the form (x,y) by guessing bits of y (including guessing when the end of y has been reached) when M needs them. M' also keeps a counter and if M tries to read more than $r(|x|)$ bits of y, then M' will reject the input x for this series of guesses. If M rejects (x,y), then M' will also reject x on the corresponding computation path. If M accepts then M' will continue to guess bits of y, and it accepts when it guesses that the end has been reached; again if it tries to exceed $r(|x|)$ total bits of y then it rejects.

We also require that every guess made by M' be actually "written down" when made (at least temporarily) so that distinct values of y satisfying $R(x,y)$ and $|y| \leq r(|x|)$ will cause M' to follow distinct computation paths. Clearly there is a polynomial q such that M' on any input x and any computation path, halts in at most $q(|x|)$ steps; by standard techniques, we can actually assume that any computation of M' that accepts x halts in exactly $q(|x|)$ steps.

Now M' is coded into (SAT,s) as in Simon [Si]. In order to show $(R,r) \leq (SAT,s)$ we obtain the required mappings as follows:

1. $f(x)$ is the Boolean formula obtained by coding the computations of M' on the input x;

2. $g(x,y)$ is anything we like if $|y| > r(|x|)$; otherwise, let M' operate on input x and guess precisely the input y when simulating the machine M: then let $g(x,y)$ be the Boolean assignment to the variables of the formula $f(x)$ which describes this computation.

We may now assert that these functions have the required properties. Properties 1. and 2. of the definition of $\leq^P$ are clear. For 3., we must show that

$$\left[R(x,y) \wedge |y| \leq r(|x|)\right] \text{ implies } \left[S(f(x),g(x,y)) \wedge |g(x,y)| \leq s(|f(x)|)\right].$$

But this should be clear from the construction of M', f(x) and g(x,y). To see 4., suppose that $R(x,y_1)$, $R(x,y_2)$, $|y_1| \leq r(|x|)$, $|y_2| \leq r(|x|$, and $g(x,y_1) = g(x,y_2)$ are all true. Since M' writes down all its guesses, it must be the case that $y_1 = y_2$.

Finally we will show 5. Suppose that $S(f(x),z)$ and $|z| \leq s(|f(x)|)$ are true. Since z encodes the guesses of M', there must be an input y (since M' only guesses the second input) such that $R(x,y)$ with $|y| \leq r(|x|)$ and by construction $g(x,y) = z$. Thus g is onto, and hence (SAT,s) is P-complete. ⊠

We could, of course, extend Proposition 2 to a collection of other polynomial-computable relations. Rather than pursuing such results, we turn our attention to relations computable by logspace combination machines. Let GAP(x,y) be "x encodes an acyclic directed graph (Savitch [Sa]) with the partial ordering induced by the edge directions consistent with the total ordering induced by the node numbering, and y encodes a directed path from start to finish." Again let $s(n) = n$. Clearly, GAP is computable by a logspace combination machine.

Proposition 3: (GAP,s) is L-complete.

Proof: Since this is almost identical to the proof of Proposition 2 we will only sketch it. Let R be a relation computable by a logspace combination machine M, and let r be a polynomial. Define M' as follows:

> M' on input x simulates M on inputs of the form (x,y) by guessing bits of y when M needs them. (Note since M is 1-way on this input M' does not have to remember all of y). M' then operates just as in Proposition 2.

Since guesses need only be written down temporarily, there is no difficulty with the space bound. Clearly M' will be a nondeterministic logspace Turing machine which we can assume halts for any computation in exactly $q(|x|)$ steps, for some polynomial q.

M' is encoded into GAP as in [Sa]. Then f and g are obtained as follows:

(1) f(x) is the graph obtained by encoding of M' on x.

(2) g(x,y) is anything we like if $|y| > r(|x|)$. Otherwise, let M' on input x with guesses y yield the path g(x,y) through the graph f(x).

Then $(R,r) \leq^{L} (SAT,s)$ via this f and g. A key again is that the computation of M' encodes the actual y it guesses so that g(x,y) will be 1-1. ⊠

We note that Proposition 3 is also extendible to a variety of other logspace computable relations.

3. Size of Solution Sets for Relations

We consider L-complete (P-complete) (R,r). We wish to give a complexity classification for

$$(R,r)_k = \{x \mid \exists \text{ exactly k values of } y,\ |y| \leq r(|x|) \wedge R(x,y)\}$$

for various values of k. We will first examine specific problems and then we will use the results of Section 2 to obtain generalizations. In the following, we let $\leq_m^P$, $\leq_m^L$, $\leq_T^P$ and $\leq_T^L$ represent the reducibilities used by Karp [K], Jones and Laaser [JL], Cook [C] and Ladner and Lynch [LaL], respectively. For convenience, we let SAT1(x,y) be "x is an arbitrary form Boolean formula and y is an assignment of true or false to the variables of x making x true." Let s(n) = n as before. Then it is clear that (SAT1, s) is P-complete.

Proposition 4: For any fixed $k \geq 1$,

(a) $(SAT1,s)_k \overset{P}{\underset{m}{\equiv}} (SAT1,s)_1$, and

(b) $(GAP,s)_k \overset{L}{\underset{m}{\equiv}} (GAP,s)_1$.

Proof: (a) We first show $(SAT1,s)_k \overset{P}{\underset{m}{\leq}} (SAT1,s)_1$. If x is not a Boolean formula, define f(x) = x. Otherwise, assume x is of the form $a(x_1,\ldots,x_n)$. Let f(x) be the formula obtained by selecting new disjoint sets of variables $\{x_{i1},\ldots,x_{in}\}_{i=1}^{k}$ and expanding into the appropriate form the expression:

$$\Big[a(x_{11},\ldots,x_{1n}) \wedge a(x_{21},\ldots,x_{2n}) \wedge \cdots \wedge a(x_{k1},\ldots,x_{kn})$$

$$\wedge (x_{11}x_{12}\cdots x_{1n} < x_{21}x_{22}\cdots x_{2n} < \cdots < x_{k1}x_{k2}\cdots x_{kn})\Big]$$

The last line of inequalities is intended to indicate lexicographic ordering of the given strings. f is computable in polynomial time, and x has exactly k solutions iff f(x) has exactly 1 solution.

Next we show $(SAT1,s)_1 \overset{P}{\underset{m}{\leq}} (SAT1,s)_k$. If k=1 there is nothing to prove, so assume $k \geq 2$. If x is not a Boolean formula, define f(x)=x. Otherwise, assume x is of the form $a(x_1,\ldots,x_n)$. Let f(x) be the formula

$$\Big[a(x_1,\ldots,x_n) \wedge \bigwedge_{i=1}^{k-1} \overline{x_{n+i}}\Big]$$

$$\vee \bigvee_{i=1}^{k-1} \left[\left(\bigwedge_{j=1}^{n+i} x_j\right) \wedge \left(\bigwedge_{j=n+i+1}^{n+k-1} \overline{x_j}\right)\right].$$

f essentially adds k-1 dummy solutions to x, and so x has exactly 1 solution iff f(x) has exactly k solutions.

(b) We first show $(GAP,s)_k \overset{L}{\underset{m}{\leq}} (GAP,s)_1$. Assume $k \geq 2$. If x is

not an acyclic directed graph satisfying the given consistency condition, then let $f(x)=x$. Otherwise, let $p: N^k \times \{0,1\}^{k-1}$ be a natural 1-1 2k-1-tupling function with the property that

$$\left[\bigwedge_{i=1}^{k} (x_i \leq y_i) \wedge \bigvee_{i=1}^{k} (x_i < y_i)\right] \text{ implies}$$

$$p(x_1,\ldots,x_k,a_1,\ldots,a_{k-1}) < p(y_1,\ldots,y_k,b_1,\ldots,b_{k-1}).$$

The start node of $f(x)$ is $(\underbrace{n_s,\ldots,n_s}_{k},\underbrace{0,\ldots,0}_{k-1})$,

where n_s is the start node of x. The goal node of $f(x)$ is $(\underbrace{n_G,\ldots,n_G}_{k},\ \underbrace{1,\ldots,1}_{k-1})$, where n_G is the goal node of x. The edges of graph $f(x)$ will be defined by tupling together edges of x as follows:

$$(p(x_1,\ldots,x_k,a_1,\ldots,a_{k-1}),\ p(y_1,\ldots,y_k,b_1,\ldots,b_{k-1}))$$

will be an edge of $f(x)$ exactly if:

(1) $(x_1,\ldots,x_k,a_1,\ldots,a_{k-1}) \neq (n_G,\ldots,n_G,1,\ldots,1)$, and

(2) for all i, $1 \leq i \leq k-1$,

(a) either (x_i,y_i) is an edge of x, or $x_i=y_i=n_G$, and
(b) one of (b1) - (b3) holds:

(b1) $a_i=0$ and $x_i=x_{i+1} \neq n_G$ and $b_i=0$ and $y_i=y_{i+1} \neq n_G$,

(b2) $a_i=0$ and $x_i=x_{i+1} \neq n_G$ and $b_i=1$ and $y_i < y_{i+1}$,

(b3) $a_i=1$ and $b_i=1$.

The reader may verify that f(x) is an acyclic directed graph satisfying the given consistency condition, and that f(x) is computable from x in logspace. Intuitively, a single path through f(x) corresponds to parallel simulation of k distinct paths through x, where a flag is changed from 0 to 1 to indicate that two "adjacent" paths have just been discovered to diverge (with the path at the left preceding the path at the right lexicographically. Padding is used for shorter paths in x. With this intuition, the reader should be able to verify that x has exactly k solutions iff f(x) has exactly 1 solution.

Finally, we must show $(GAP,s)_1 \leq_m^L (GAP,s)_k$. But this is straightforward by a construction which adds k-1 disjoint "dummy paths" to a graph of the appropriate type. ⊠

We now note that a result similar to Proposition 4. must hold for <u>all</u> complete (R,r). That is, addition of dummy solutions and collapsing of several solutions to one are constructions which work for all complete problems. In fact, all such problems must be equivalent to each other:

<u>Proposition 5</u>: For any fixed $k \geq 1$,

(a) if (R,r) is P-complete, then $(R,r)_k \equiv_m^P (SAT1,s)_1$, and

(b) if (R,r) is L-complete, then $(R,r)_k \equiv_m^L (GAP,s)_1$.

<u>Proof</u>: By Proposition 4. and the fact that our reducibilities $\leq_m^L$ and $\leq_m^P$ preserve cardinality of solution sets (as noted immediately prior to Proposition 1). ⊠

Now that we know that all size problems lie in a common complexity class, we would like to be able to say more about the location of this class. The only such information we have so far arises as a result of the following Proposition. Here, let S=

$\{x|\ \exists y\ \ |y| \leq s(|x|) \wedge SAT1\ (x,y)\}$ and let

$G = \{x|\ \exists y\ \ |y| \leq s(|x|) \wedge GAP\ (x,y)\}$, i.e. nondeterministic problems of the usual sort.

Proposition 6:

(a) If $\bar{S} \underset{m}{\leq}^{P} A \leq_{T}^{P} S$, then

$A \in NP$ iff NP is closed under complement, and

$A \in P$ iff $P=NP$, and

(b) if $\bar{G} \underset{m}{\leq}^{L} A \leq_{T}^{L} G$, then

$A \in NL$ iff NL is closed under complement, and

$A \in L$ iff $L=NL$.

Proof: The arguments are all standard Turing machine constructions, of the type found in [JL] or [LaL], for example. ⊠

Finally, we can conclude:

Proposition 7: For any fixed $k \geq 1$,

(a) if (R,r) is P-complete, then

$(R,r)_k \in NP$ iff NP is closed under complement, and

$(R,r)_k \in P$ iff $P=NP$, and

(b) if (R,r) is L-complete, then

$(R,r)_k \in NL$ iff NL is closed under complement, and

$(R,r)_k \in L$ iff $L=NL$.

Proof:

(a) Because of Propositions 5. and 6., it suffices to show $\bar{S} \leq_m^P (SAT1,s)_1 \leq_T^P S$. To see the first reduction, we use a special case of a construction for Proposition 4(a): if x is not a Boolean formula, define f(x) = x. Otherwise, if x is of the form $a(x_1,\ldots,x_n)$ let f(x) be the formula $\left[a(x_1,\ldots,x_n) \wedge \overline{x_{n+1}}\right] \vee \left[x_1 \wedge \ldots \wedge x_n \wedge x_{n+1}\right]$.

x has no solutions iff f(x) has exactly one solution.

To see the second reduction, note that $(SAT1,s)_1 = A \cap \bar{B}$, where

$A = \{x \mid \exists$ at least k values of y, $|y| \leq s(|x|) \wedge SAT1(x,y)\}$

$B = \{x \mid \exists$ at least k+1 values of y, $|y| \leq s(|x|) \wedge SAT1(x,y)\}$.

Clearly A,B are both in NP, so that $A \leq_m^P S$ and $B \leq_m^P S$. Then a Turing machine with an S-oracle may easily be constructed to decide membership in $(SAT1,s)_1$.

(b) It suffices to show $\bar{G} \leq_m^L (GAP,s)_1 \leq_T^L G$.

The first reduction follows by adding a single "dummy path" to a graph. The second follows from the same argument as in (a). ⊠

Of course, the given complexity classification is still very incomplete; further work remains to be done.

We would expect that there are other interesting properties of solution sets which are preserved by strong reducibilities such as ours. Finding the appropriate strength reducibilities needed to preserve constructions such as those used for approximation, or for finding a <u>particular</u> solution when existence is known, seems to be an interesting area for further study.

[C] Cook, S. A. The Complexity of Theorem-Proving Procedures. Proc. 3rd ACM Symposium in Theory of Computing, 1971, pp. 151-158.

[JL] Jones, N. and Laaser, W. Complete problems for deterministic polynomial time, Proceedings of Sixth Annual ACM Symposium on Theory of Computing, April-May 1974, pp. 40-46.

[K] Karp, R. M. Reducibility Among Combinaterial Problems. In Complexity of Computer Computations (R. Miller and J. Thatcher, ed.) Plenum Press, 1972, pp. 85-104.

[LaL] Ladner, R. and Lynch, N. A. Relativization of Questions About Log Space Computability; Math Systems Theory 10, (1976) pp. 19-32.

[LiL] Lipton, R. and Lynch, N. A. A Quantifier Characterization for Nondeterministic Log Space, SIGACT News, December 1975, Volume 7, No. 4, pp. 24-26.

[Sa] Savitch, W. Relations Between Nondeterministic and Deterministic Tape Complexities, JCSS Vol. 14, 1970 pp. 177-192.

[Si] Simon, J. On Some Central Problems in Computational Complexity, Cornell University TR 75-224, 1975.

[SM] Stockmeyer, L. and Meyer, A. R. Word Problems Requiring Exponential Time: Preliminary Report, 5th Annual ACM Symposium on Theory of Computing 1973, pp. 1-9.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 85	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) On Structure Preserving Reduction		5. TYPE OF REPORT & PERIOD COVERED Technical
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Richard J. Lipton Nancy Lynch		8. CONTRACT OR GRANT NUMBER(s) N00014-75-C-0752
9. PERFORMING ORGANIZATION NAME AND ADDRESS Yale University Department of Computer Science 10 Hillhouse Ave, New Haven, CT 06520		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Office of Naval Research Information Systems Program Arlington, Virginia 22217		12. REPORT DATE DEC 1976 13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Distribution of this report is unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

reduction
polynomial time
logspace
complete sets

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The concept of reduction between problems is strengthened. Certain standard problems are shown to be complete in the new and stronger sense. Applications to the number of solutions of particular problems are presented.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)